Secure Shell

Category: Security & Logging In

The SSH protocol is used for both interactive login sessions and executing arbitrary commands on remote systems. It provides secure, encrypted communication between two untrusted hosts over an insecure network. Users must prove their identities to successfully connect to a remote system. Both the authentication information, such as a password or passcode, as well as data are encrypted over the network.

SSH uses a client-server model. On the client, users initiate an SSH connection with the *ssh* command, which connects to the *sshd* daemon on the remote system.

OpenSSH

All NAS systems, except the secure front-ends, use the OpenSSH implementation of the SSH protocol.

This implementation includes *ssh, scp, sftp, sshd,* and utilities such as *ssh-add, ssh-agent,* and *ssh-keygen*. On the secure front-ends, a commercial implementation of the SSH server is used, but OpenSSH is used for the SSH client.

Although OpenSSH includes support for both SSH protocol 1 and protocol 2, all NAS systems accept only connections using protocol 2.

Please be aware that there are both security and performance issues with older versions of OpenSSH. NAS users are strongly recommended to use **OpenSSH 5.2 or later** for best performance, security, and functionality.
Both Mac OS X and most Linux distributions include a version of OpenSSH. However, it is important to keep up with the latest security updates for your operating system to ensure that you have the latest version of OpenSSH supported by the vendor.

On systems running the Windows operating system, please ensure that a client supporting SSH protocol 2 is installed. We recommend using Cygwin (a Linux-like environment for Windows) and OpenSSH. Follow the instructions in the PDF file Installing cygwin/openssh for more details.

To learn more about OpenSSH, see the **ssh(1)** and **ssh_config(5)** man pages.

The following Wikipedia pages have additional information on SSH:

- http://en.wikipedia.org/wiki/Secure_Shell

- http://en.wikipedia.org/wiki/OpenSSH
- http://en.wikipedia.org/wiki/Cygwin

Article ID: 228
Last updated: 11 Oct, 2011
The HEC Environment -> Security & Logging In -> Secure Shell
http://www.nas.nasa.gov/hecc/support/kb/entry/228/?ajax=1